System Vulnerability Analysis with the Network Visualization Tool (NVT)[1]

Ronda R. Henning[2]
Kevin L. Fox, Ph.D.[2]

Next generation information systems and infrastructures apply the concept of acceptable risk to vulnerability assessment and coalition information sharing. The security features of the system architecture provide sufficient protection for the mission and data processed. In previous generations of systems, a risk adverse vulnerability posture dictated custom hardware and software solutions and minimal coalition data interchange. There are few system architecture design tools available to analyze architecture alternatives among security risk, system performance, and mission functionality while accommodating budgetary constraints. Current generation risk analysis tools provide single vendor monolithic solutions that address a particular aspect of risk, but are not easily expanded to address emerging technologies and their vulnerabilities.

For the past two years, Harris Corporation has been conducting research for the U.S. Air Force Research Laboratory under the Network Vulnerability Tool (NVT) Study. The Network Vulnerability Tool concept uses a single topological model to support the information needs of multiple vulnerability analysis tools through a knowledge solicitation and translation framework. As part of this effort, existing COTS, GOTS, and research laboratory vulnerability assessment tools were surveyed, and a representative sample of tools was selected for inclusion in the NVT prototype. The prototype integrates and interactively applies multiple existing vulnerability assessment technologies, to produce a cohesive, combined vulnerability/risk assessment. This helps the analyst define an acceptable risk posture for a deployed or preliminary system design. NVT defines a preliminary vulnerability assessment environment, consolidating multi-source output into a cohesive visual vulnerability assessment capability.

This functionality can be used as a tool to:

- identify vulnerabilities in systems early in the development process,
- baseline the security configuration of a developed system,
- trace security configuration changes over the system lifecycle, and
- facilitate "defense in depth" security perimeter definition activities.

This presentation describes the NVT development effort, and some preliminary results from using the tool.

EXHIBIT 2

[1] This research has been entirely funded under the Network Visualization Tool (NVT) program for U.S. AFRL/IFGB, contract #F30602-96-C-0289.

[2] Harris Information Systems Division, P.O. Box 98000, 150 S. Wickham Road, Melbourne, FL 32902.